# Challenges of Security Feature Adoption

## Michael Condry

## Senior Security Technologist

## Intel Corporation

# Agenda

**Situation**

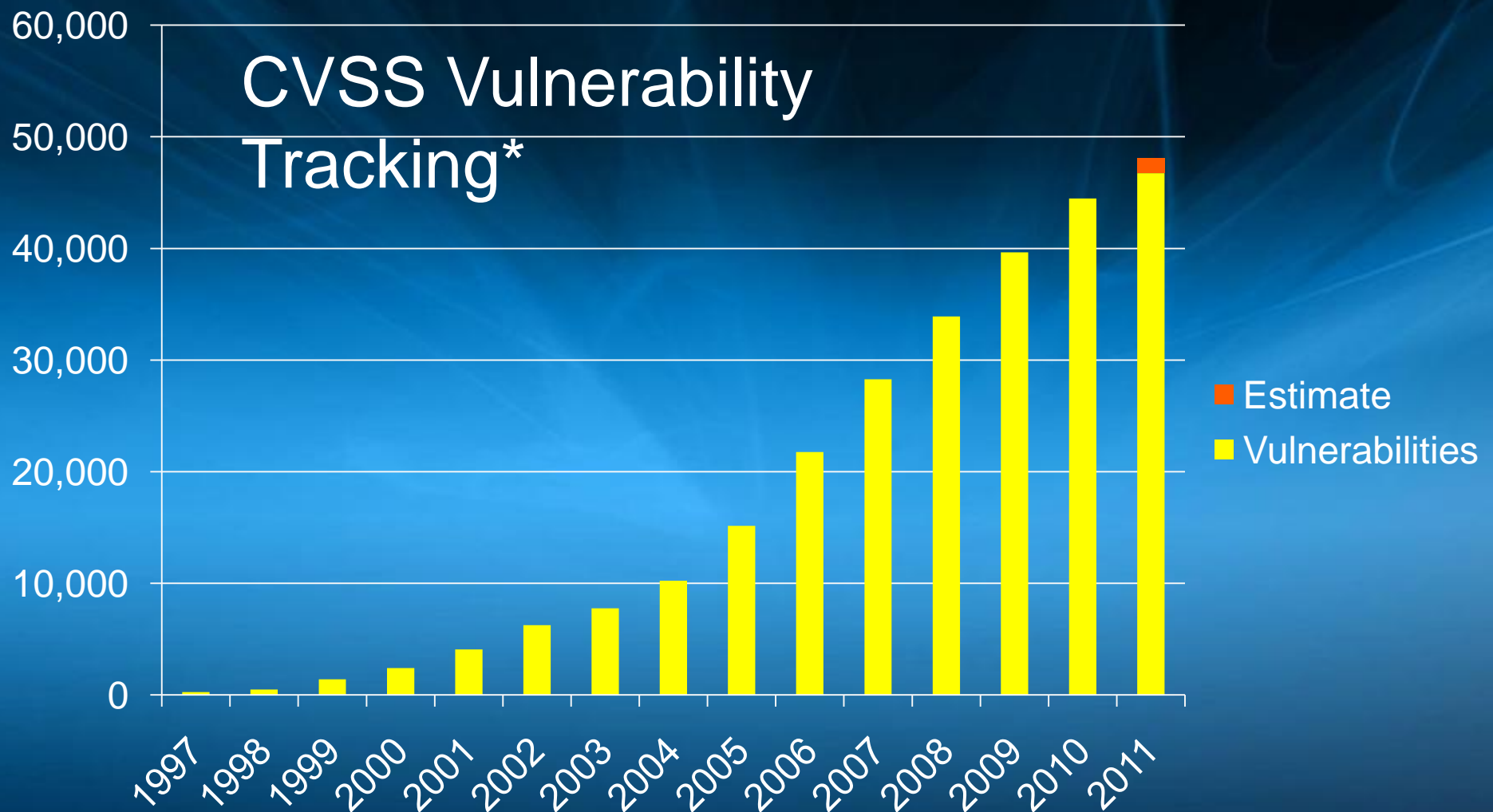**Exposure and Costs**

**Security Adoption Complexities**

**Discussion**

# Situation: Security Adoption is a Problem

- Security is an "End to End" problem
  - System vendors provide some technology elements
  - Software and Service vendors provide some elements
  - End user must adopt and "turn on" the security features
  - The End user is typically the "weakest link" in the security ecosystem

- End user scope includes many devices
  - Traditional compute engine (PC, Mac, …)
  - Cloud and Servers
  - Mobile Smart Phones and Tablets
  - Control Systems, automobiles, ….
- An end user device can access enterprise or control systems
- Security feature that is not adopted end to end is not security

# Vulnerabilities Grow Daily

CVSS Vulnerability Tracking*

Legend:
- ■ Estimate
- ■ Vulnerabilities

Chart x-axis years: 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011

Chart y-axis: 0, 10,000, 20,000, 30,000, 40,000, 50,000, 60,000

Growth of Software alone > 5K Year over Year

* Source NIST

Slide 4

# Exposures Can Be Long*

## Days to Resolve

| Category | Days to Resolve |
|---|---|
| Virus, worms, trojans | ~2 |
| Botnets | ~2 |
| Malware | ~3.5 |
| Phishing | ~9 |
| Stolen Devices | ~11 |
| Denial of Service | ~13 |
| Web-based Attacks | ~23 |
| Malicious Code | ~41 |
| Malicious Insiders | ~45 |
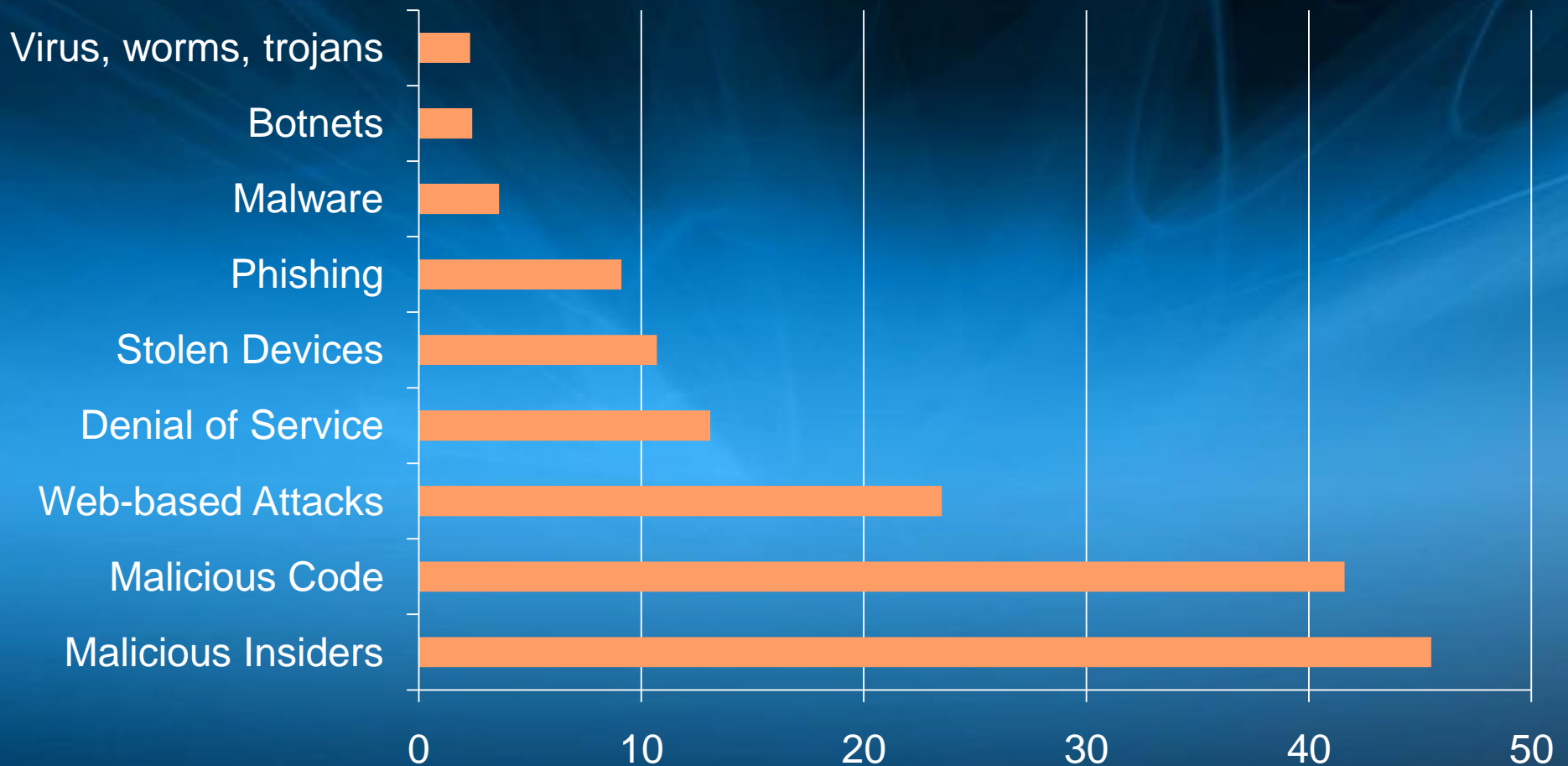
*Source: Ponemon Institute Study, August 2011 – 50 organization study
Note: Resolve is time from discovery to point the situation is declared contained

# Who Cares About Security

- **IT** needs to protect assets:
  - 35% CAGR 2010-2014 Mobile security alone
- **SMB** – needs security with no IT staff/skills
  - Neustar shows 75% SMB would fail with a DOS attack on their sites
- **Cloud Computing**:
  - Visa estimates on-line fraud> $2.7 B in 2010 – Reuters January 2011
- ISVs:
  - IDC 2009 report shows $55B loss in Software piracy
- Many Others:
  - Retail, Banking, Government, Social Media, Control Systems, Factories
- **Consumers** want security but do not understand it enough to worry, until they lose. They create the "the weakest link"
  - Despite news reports, ID thefts, auto thefts, …

# Areas of Security Technologies

**Identity Protection & Fraud Deterrence**

*Access to your systems & services is more secure*

**Detection & Prevention of Malware**

*Defending you against hidden Trojans, etc*

**Securing Media, Data and Assets**

*Protect your valuable data & assets from theft or loss*

**Recovery, Patching and Upgrading**

*Quickly recover from an attack*

# Adoption Complexities

- Industry (and Government)
  - Cloud access convenience vs. lack of device control

- End Users
  - Lack of adoption due mainly to lack of value understanding, Facebook™ sharing more understandable
  - Social Networking often leads to security exposures via leaks

- Vendors/Providers
  - Industry wide accepted security Impact Metrics unavailable
  - Feature providers do not always consider cross ecosystem costs
  - Legacy systems not always considered
  - Too awkward usage results in non-consumer adoption
  - Market requires multiple device solutions
  - Product support, updates, recovery and upgrades often too short or non-existent
  - Target customer confusion over offering

IEEE
Advancing Technology
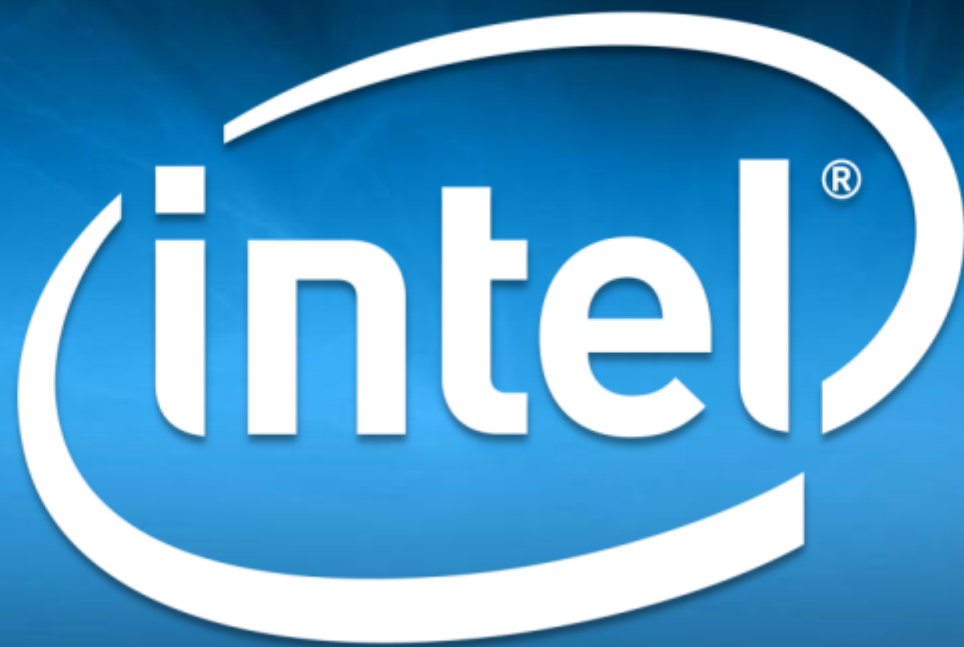for Humanity

intel

# Vendor Area Examples Solutions

| Area | Strong | Middle | Weak |
|------|--------|--------|------|
| Impact Measurement | Industry Standard Comparison or Benchmark | Vulnerability or Independent Analysis | "Trust Me" |
| Cost Factors | OxM/BIOS no BOM ISV/OSV Common Code Base – separate SDK & Library | OxM/BIOS minimum BOM and validation | OxM/BIOS major (change or validation) Separate Codes |
| Legacy | Package allows legacy "to work" – new HW is better | Legacy is has minor transition, but things "sorta work" | Ignore Legacy |
| Consumer | Minimize interface overhead, open to multiple platforms | Give and Take; Usable but with issues | Force service and design; awkward usage |
| Market | Multiple Device Considerations | Selected continuum devices | Unique Platform Solution |
| Support | Well defined Update and Upgrade strategy | Limited Update options | No update considerations |
| Usage Complexity | Easy to use and understand | Limited usability challenges | Confusing for End User |

# Discussion

- Where do you see Adoption Challenges?
- Do you agree that lack of adoption "end to end" in the ecosystem creates a major exposure even for the control industry?
- How to address growing Social Networking impacts?
- Can we cooperate to scope standard Adoption Criteria?
- How to push Industry Accepted Metrics, Benchmarks and Brands?
- How to find an *acceptable* way to assist the consumer in value understanding and adoption of security?
  - The "weakest link" needs suitable assistance they can use

# IEEE Security Ranking